UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/694,925	10/27/2003	Justin Monk	020375-043600US	5092

20350 7590 01/05/2009
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
THEIN, MARIA TERESA T	

ART UNIT	PAPER NUMBER
3627	

MAIL DATE	DELIVERY MODE
01/05/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/694,925
Filing Date: October 27, 2003
Appellant(s): MONK, JUSTIN

Daniel J. Sherwinter
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed October 21, 2008 appealing from the Office action mailed May 16, 2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,649,118	CARLISLE ET AL.	7-1997
5,796,832	KAWAN	8-1997

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7 and 23-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carlisle et al. in view of Kawan.

Carlisle et al. shows all of the limitations of the claims except for specifying a remote host.

Carlisle et al. shows an improved systems and methods applicable to smart cards in a point-of-sale environment are described in FIGS. 1-14. In general, the point-of-sale transactions work in the following manner. A card holder (i.e., a consumer) selects a plurality of consumer items to be purchased and brings them to a point-of-sale configuration which includes a smart card reader. The consumer items each include a conventional Universal Price Code (UPC) bar code identifier, which may be conceptualized as an item identifier. The consumer inserts the smart card into the smart card reader, thereby activating a sequence of operations for debiting a plurality of accounts. The operational sequence implements the following functions. The Universal Price Code (UPC) of the consumer item to be purchased, i.e., the item identifier, is read by an item identification device, for example, by scanning the bar code of the item or by entering the code manually into a keypad at the point-of-sale terminal. Based upon the UPC code and one or more application identifiers held on the smart card, the point-of-sale terminal compares the UPC against item tables stored in memory which identify the item's eligibility for debit against one or more of the card holder's accounts. If an item is eligible for more than one account, a debit priority algorithm determines which of the accounts should be debited. The debit priority algorithm may utilize one or more debt allocation tables which, for each of a plurality of item identifiers, sets forth a priority ranking for a plurality of accounts. The comparison of item UPC codes for purchased items to UPC codes stored in the item arrays can be done as the UPC code of each item is entered at the point-of-sale terminal. Alternatively, UPC codes for each individual item can be buffered until all items for a given point-of-sale transaction are entered. The individual items are then debited into individual accounts. Additionally, the card holder is provided with the ability to mix account balance categories (dollars, specific item identification, item quantity, etc.) on a single card for a single transaction corresponding to a plurality of accounts. The functions described in the previous paragraphs will be described in greater detail hereinafter. First, the software operating system of the smart card will be considered.

Kawan teaches a wireless transaction and information system where the smart card and a remote host work in concert together in order to improve security.

Based on the teaching of Kawan, it would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the Carlisle et al. invention to incorporate the remote host of Kawan in order to improve security.

(10) Response to Argument

Appellant remark that "the newly cited art still fails to teach or suggest linking a single identifier of a payment instrument to multiple accounts at a remote host, and using that remote host to generate account information based on the instrument identifier for use in point-of-sale transactions with the instrument, as recited in independent claims 1 and 30". (Argument section, page 6, first paragraph)

The Examiner does not agree. The combination of Carlisle and Kwan teaches or suggest the recitation above. Carlisle discloses a smart card wherein plurality of accounts is stored (abstract) and is used in a point-of-sale transaction (col. 3, lines 37-38). The smart card contains an electronic purse that will hold a monetary value (col. 13, lines 14-15) and accounts which are implemented by service providers such as Visa, MasterCard, ATM networks, welfare programs, or the like (col. 2, lines 27-30). The smart card operating system includes a read-only memory (ROM) which contains the commands/modules/files that effect writing to a file (col. 6, lines 65-67). The writing to a file is restricted to whatever the owner of the file specifies (the owner of a file is initially, the user that crates the files) (col. 7, lines 1-3). Other items that are installed in the ROM or more typically in a “write once” memory (because they are unique to each smart card) are Root password and smart card’s ID information. The ID information is an arbitrary string or it may include the Holder’s name. Both the root password and smart card’s PIN (personal identification number) can be encased in the file. (Col. 7, lines 7-14) Furthermore, the operating system includes an encryption key pair that is installed in a filed owned by Root and that key pair is unique to each smart card (col. 7, lines 27-31). Carlisle further discloses a smart card point-of-sale configuration which is divided into several subsystems. The smart card contains a memory capable of storing and updating information for a user. The smart card reader/writer links the card with a point-of-sale terminal. The point-of-sale terminal is a configured application station which comprises a computer or dedicated workstation that runs application software necessary for accessing the memory in the smart card. The application software resides in a memory of the point-of-sale terminal and enables the retrieval and modification of information stored in the memory of the smart card. This memory is the random-access memory (RAM), read-only memory (ROM), or the like. The smart card runs an executable operating system that is accessed via a set of operating system commands. These commands manipulate a file system on the card in accordance with rules required by card security. (Col. 17, lines 22-42) The security process begins with the smart card’s possessor being authenticated as the bona-fide Holder of the smart card (col. 9, lines 21-23). For example in a merchant’s premises, the possessor would insert the smart card into a stand-alone reader equipment, input the PIN via the keyboard, and the equipment’s display will output the message “OK”. This will give the

Holder of the smart card a sense of security that the equipment used for transaction will not capture their PIN string for some future unlawful use. When such stand-alone equipment is unavailable (or when the communication is remote as, for example, when a “dumb” card reader is used the possessor’s home), the submitted PIN should be processed in the card and the “OK” message from the smart card should be “time-stamped” and encrypted. (Col.9, lines 21-42) Furthermore, Carlisle disclose an operating system which includes complete encrypted communication, which provides the capability of imparting confidence in remote communication, that permits remote provisioning, effective maintenance of a database that keeps track of all services contained in each smart card (col. 4, lines 37-44). Figure 8 of Carlisle discloses the remote provisioning of smart cards using the telecommunication network (col. 3, lines 18-19). The Examiner then turns to Kawan to teach an information system where the smart card and a remote host work in concert together in order to improve security. Kawan discloses a smart card and a smart card reader. The smart card includes a processing means as well as both volatile and non-volatile memory. Data stored in read-write memory on the smart card may be exchanged with a reader device, typically through a serial interface. One advantage of such use of the smart card is those encryptions algorithms may be stored and processed with the smart card to allow the smart card to be validated from a remote location, for example, by a host computer operated by a financial institution. In this way, information can be securely exchanged between the card and the remote location using one or more encryption keys that are place in both locations. (Col. 4, lines 15-30)

Such teaching of Carlisle's smart card wherein plurality of accounts is stored and is used in a point-of-sale transaction; smart card containing an electronic purse that will hold a monetary value and accounts which are implemented by service providers such as Visa, MasterCard, ATM networks, welfare programs, or the like; smart card operating system includes a read-only memory (ROM) which contains Root password and smart card's ID information that are unique to each smart card; ID information which is an arbitrary string or it may include the Holder's name; root password and smart card's PIN (personal identification number) can be encased in the file; operating system includes an encryption key pair that is installed in a filed owned by Root and that key pair is unique to each smart card; smart card reader/writer linking the card with a point-of-sale terminal; point-of-sale terminal which is a configured application station which comprises a computer or dedicated workstation that runs application software necessary for accessing the memory in the smart card; smart card runs an executable operating system that is accessed via a set of operating system commands, the commands manipulate a file system on the card in accordance with rules required by card security; security process begins with the smart card's possessor being authenticated as the bona-fide Holder of the smart card; possessor would insert the smart card into a stand-alone reader equipment, input the PIN via the keyboard, and the equipment's display will output the message "OK", thus giving the Holder of the smart card a sense of security that the equipment used for transaction will not capture their PIN string for some future unlawful use, in a merchant's premises; when stand-alone equipment is unavailable (or when the communication is remote as, for example, when a “dumb” card reader is used the possessor’s home), the submitted PIN should be processed in the card and the “OK” message from the smart card should be “time-stamped” and encrypted; operating system which includes complete encrypted communication, which provides the capability of imparting confidence in remote communication, that permits remote provisioning; with the combination of Kawan’s smart card and a smart card reader; smart card being validated from a remote location, for example, by a host computer operated by a financial institution; and the encryptions algorithms stored and processed with the smart card to allow the smart card to be validated from a remote location, thus the information can be securely exchanged between the card and the remote location using one or more encryption keys that are place in both locations are considered “linking a single identifier of a payment instrument to multiple accounts at a remote host, and using that remote host to generate account information based on the instrument identifier for use in point-of-sale transactions with the instrument”.

Appellant remarks that Carlisle and Kawan fail to teach or suggest “receiving, at the point-of-sale device from an instrument, an instrument identifier identifying the instrument, wherein the instrument identifier is associated with a stored-value account and a credit account…; transmitting, from the point-of-sale service to the remote host, the instrument identifier”. (Argument section, page 6, second paragraph)

The Examiner does not agree. The combination of Carlisle and Kwan teaches or suggest the recitation above. Carlisle discloses a smart card wherein plurality of accounts is stored (abstract) and is used in a point-of-sale transaction (col. 3, lines 37-

38). The smart card contains an electronic purse that will hold a monetary value (col. 13, lines 14-15) and accounts which are implemented by service providers such as Visa, MasterCard, ATM networks, welfare programs, or the like (col. 2, lines 27-30). The smart card operating system includes a read-only memory (ROM) which contains the commands/modules/files that effect writing to a file (col. 6, lines 65-67). Other items that are installed in the ROM or more typically in a “write once” memory (because they are unique to each smart card) are Root password and smart card’s ID information. The ID information is an arbitrary string or it may include the Holder’s name. Both the root password and smart card’s PIN (personal identification number) can be encased in the file. (Col. 7, lines 7-14) Furthermore, the operating system includes an encryption key pair that is installed in a filed owned by Root and that key pair is unique to each smart card (col. 7, lines 27-31). Carlisle further discloses a smart card point-of-sale configuration which is divided into several subsystems. The smart card contains a memory capable of storing and updating information for a user. The smart card reader/writer links the card with a point-of-sale terminal. The point-of-sale terminal is a configured application station which comprises a computer or dedicated workstation that runs application software necessary for accessing the memory in the smart card. The application software resides in a memory of the point-of-sale terminal and enables the retrieval and modification of information stored in the memory of the smart card. This memory is the random-access memory (RAM), read-only memory (ROM), or the like. The smart card runs an executable operating system that is accessed via a set of operating system commands. These commands manipulate a file system on the card in accordance with rules required by card security. (Col. 17, lines 22-42) The security process begins with the smart card's possessor being authenticated as the bona-fide Holder of the smart card (col. 9, lines 21-23). For example in a merchant's premises, the possessor would insert the smart card into a stand-alone reader equipment, input the PIN via the keyboard, and the equipment's display will output the message "OK". This will give the Holder of the smart card a sense of security that the equipment used for transaction will not capture their PIN string for some future unlawful use. When such stand-alone equipment is unavailable (or when the communication is remote as, for example, when a "dumb" card reader is used the possessor's home), the submitted PIN should be processed in the card and the "OK" message from the smart card should be "time-stamped" and encrypted. This suggest that the possessor's confirmation as the Holder must be postponed until after the appropriate encryption keys are established and date and time information is imparted to the smart card. (Col.9, lines 21-45) Furthermore, Carlisle disclose an operating system which includes complete encrypted communication, which provides the capability of imparting confidence in remote communication, that permits remote provisioning, effective maintenance of a database that keeps track of all services contained in each smart card (col. 4, lines 37-44). Figure 8 of Carlisle discloses the remote provisioning of smart cards using the telecommunication network (col. 3, lines 18-19). The Examiner then turns to Kawan to teach an information system where the smart card and a remote host work in concert together in order to improve security. Kawan discloses a smart card and a smart card reader. The smart card includes a processing means as well as both volatile and non-volatile memory. Data stored in read-write memory on the smart card may be exchanged with a reader device, typically through a serial interface. One advantage of such use of the smart card is those encryptions algorithms may be stored and processed with the smart card to allow the smart card to be validated form a remote location, for example, by a host computer operated by a financial institution. In this way, information can be securely exchanged between the card and the remote location using one or more encryption keys that are place in both locations. (Col. 4, lines 15-30)

Such teaching of Carlisle's smart card wherein plurality of accounts is stored and is used in a point-of-sale transaction; smart card containing an electronic purse that will hold a monetary value and accounts which are implemented by service providers such as Visa, MasterCard, ATM networks, welfare programs, or the like; smart card operating system includes a read-only memory (ROM) which contains Root password and smart card's ID information that are unique to each smart card; ID information which is an arbitrary string or it may include the Holder's name; root password and smart card's PIN (personal identification number) which can be encased in the file; operating system includes an encryption key pair that is installed in a filed owned by Root and that key pair is unique to each smart card; smart card reader/writer linking the card with a point-of-sale terminal; point-of-sale terminal which is a configured application station which comprises a computer or dedicated workstation that runs application software necessary for accessing the memory in the smart card; smart card runs an executable operating system that is accessed via a set of operating system commands, the commands manipulate a file system on the card in accordance with rules required by card security; security process begins with the smart card's possessor being authenticated as the bona-fide Holder of the smart card; possessor would insert the smart card into a stand-alone reader equipment, input the PIN via the keyboard, and the equipment's display will output the message "OK", thus giving the Holder of the smart card a sense of security that the equipment used for transaction will not capture their PIN string for some future unlawful use, in a merchant's premises; when such stand-alone equipment is unavailable (or when the communication is remote as, for example, when a "dumb" card reader is used the possessor's home), the submitted PIN should be processed in the card and the "OK" message from the smart card should be "time-stamped" and encrypted; operating system which includes complete encrypted communication, which provides the capability of imparting confidence in remote communication, that permits remote provisioning; with the combination of Kawan's smart card and a smart card reader; allowing the smart card to be validated from a remote location, for example, by a host computer operated by a financial institution; and the encryptions algorithms stored and processed with the smart card to allow the smart card to be validated from a remote location, thus the information can be securely exchanged between the card and the remote location using one or more encryption keys that are place in both locations are considered "receiving, at the point-of-sale device from an instrument, an instrument identifier identifying the instrument, wherein the instrument identifier is associated with a stored-value account and a credit account…; transmitting, from the point-of-sale service to the remote host, the instrument identifier".

Appellant remarks that Carlisle and Kawan fail to teach or suggest “receiving, at the point-of-sale device from the remote host, account information relating to the stored-value account and the credit account linked to the instrument identifier, the account information being generated by the remote host based on the instrument identifier”. (Argument section, page 7, third paragraph)

The Examiner does not agree. The combination of Carlisle and Kwan teaches or suggest the recitation above. Carlisle discloses a smart card wherein plurality of accounts is stored (abstract) and is used in a point-of-sale transaction (col. 3, lines 37-38). Carlisle also discloses encryption which ensures secure communication, wherein the smart card's owner can have confidence in remote installation of services. The smart card owner must first log in into the smart card. (Col. 9, lines 14-20) The security process begins with the smart card’s possessor being authenticated as the bona-fide Holder of the smart card (col. 9, lines 21-23). For example in a merchant’s premises, the possessor would insert the smart card into a stand-alone reader equipment, input the PIN via the keyboard, and the equipment’s display will output the message “OK”. This will give the Holder of the smart card a sense of security that the equipment used for transaction will not capture their PIN string for some future unlawful use. When such stand-alone equipment is unavailable (or when the communication is remote as, for example, when a “dumb” card reader is used the possessor’s home), the submitted PIN should be processed in the card and the “OK” message from the smart card should be “time-stamped” and encrypted. (Col.9, lines 21-42) Once logged in, the holder of the smart card can communicate a request for installation of a service offered by a service provider (col. 10, lines 51-52). The service provider logs in when a possessor of a smart card established communication between the smart card and the service provider (col. 11, lines 33-36). The service request can be the holder of the smart card requesting the service provider to install money into the smart card (col. 11, lines 46-50). The smart card contains an electronic purse that will hold a monetary value (col. 13, lines 14-15) and accounts which are implemented by service providers such as Visa, MasterCard, ATM networks, welfare programs, or the like (col. 2, lines 27-30). Furthermore, Carlisle disclose an operating system which includes complete encrypted communication, which provides the capability of imparting confidence in remote communication, that permits remote provisioning, effective maintenance of a database that keeps track of all services contained in each smart card (col. 4, lines 37-44). Figure 8 of Carlisle discloses the remote provisioning of smart cards using the telecommunication network (col. 3, lines 18-19). The Examiner then turns to Kawan to teach an information system where the smart card and a remote host work in concert together in order to improve security. Kawan discloses a smart card and a smart card reader. (Col. 4, lines 15-19) Kawan further teaches various services to the customer, such as providing account information and account debiting and crediting at the customer's request. A communication front end is used to exchange data corresponding to such information. The communication front end provides access to the host computer operated by the financial institution from a variety of communication systems. (Col. 3, lines 9-15) The communication front may be connected to a network service provider or a private network. The network can be a local area networks or wide area networks. (Col. 3, lines 28-34) The smart card uses encryptions algorithms which may be stored and processed with the smart card to allow the smart card to be validated form a remote location, for example, by a host computer operated by a financial institution. In this way, information can be securely exchanged between the card and the remote location using one or more encryption keys that are place in both locations. (Col. 4, lines 23-30) A user may insert a smart card into the smart card reader. The card first encrypts, and then transmits to the terminal information stored on a smart card. This information identifies the financial institution which maintains the user's account as well as the user's account number. (Col. 5, lines 1-5)

Such teaching of Carlisle's smart card wherein plurality of accounts is stored and is used in a point-of-sale transaction; encryption which ensures secure communication, wherein the smart card's owner can have confidence in remote installation of services; possessor inserting the smart card into a stand-alone reader equipment, inputting the PIN via the keyboard, and the equipment's display will output the message “OK”, thus giving the Holder of the smart card a sense of security that the equipment used for transaction will not capture their PIN string for some future unlawful use and when such stand-alone equipment is unavailable (or when the communication is remote as, for example, when a “dumb” card reader is used the possessor's home), the submitted PIN should be processed in the card and the “OK” message from the smart card should be “time-stamped” and encrypted; logging in, wherein the holder of the smart card can communicate a request for installation of a service offered by a service provider, wherein the service request can be the holder of the smart card requesting the service provider to install money into the smart card ; the smart card which contains an electronic purse that will hold a monetary value and accounts which are implemented by service providers such as Visa, MasterCard, ATM networks, welfare programs, or the like; with the combination of Kawan’s smart card and a smart card reader; allowing the smart card to be validated from a remote location, for example, by a host computer operated by a financial institution; various services to the customer, such as providing account information and account debiting and crediting at the customer’s request, wherein a communication front end is used to exchange data corresponding to such information; communication front end provides access to the host computer operated by the financial institution from a variety of communication systems; communication front may be connected to a network service provider or a private network, such as a local area networks or wide area networks; and user inserting a smart card into the smart card reader, wherein the card first encrypts, and then transmits to the terminal information stored on a smart card, the information identifies the financial institution which maintains the user's account as well as the user's account number are considered “receiving, at the point-of-sale device from the remote host, account information relating to the stored-value account and the credit account linked to the instrument identifier, the account information being generated by the remote host based on the instrument identifier”.

Appellant remarks that “the Office Action cites no specific reference in any art as teaching or suggesting wherein the stored-value account and the credit account were linked to the instrument identifier at a remote host".

The Examiner does not agree. The combination of Carlisle and Kwan teaches or suggest the recitation above. Carlisle discloses a smart card wherein plurality of accounts is stored (abstract) and is used in a point-of-sale transaction (col. 3, lines 37-38). Carlisle also discloses encryption which ensures secure communication, wherein the smart card's owner can have confidence in remote installation of services. The smart card owner must first log in into the smart card. (Col. 9, lines 14-20) The security process begins with the smart card's possessor being authenticated as the bona-fide Holder of the smart card (col. 9, lines 21-23). For example in a merchant's premises, the possessor would insert the smart card into a stand-alone reader equipment, input the PIN via the keyboard, and the equipment's display will output the message "OK". This will give the Holder of the smart card a sense of security that the equipment used for transaction will not capture their PIN string for some future unlawful use. When such stand-alone equipment is unavailable (or when the communication is remote as, for example, when a "dumb" card reader is used the possessor's home), the submitted PIN should be processed in the card and the "OK" message from the smart card should be "time-stamped" and encrypted. (Col.9, lines 21-42) Once logged in, the holder of the smart card can communicate a request for installation of a service offered by a service provider (col. 10, lines 51-52). The service request can be the holder of the smart card requesting the service provider to install money into the smart card (col. 11, lines 46-50). The smart card contains an electronic purse that will hold a monetary value (col. 13, lines 14-15) and accounts which are implemented by service providers such as Visa, MasterCard, ATM networks, welfare programs, or the like (col. 2, lines 27-30).

Furthermore, Carlisle disclose an operating system which includes complete encrypted communication, which provides the capability of imparting confidence in remote communication, that permits remote provisioning, effective maintenance of a database that keeps track of all services contained in each smart card (col. 4, lines 37-44). Figure 8 of Carlisle discloses the remote provisioning of smart cards using the telecommunication network (col. 3, lines 18-19). The Examiner then turns to Kawan to teach an information system where the smart card and a remote host work in concert together in order to improve security. Kawan discloses a smart card and a smart card reader. The smart card uses encryptions algorithms which may be stored and processed with the smart card to allow the smart card to be validated from a remote location, for example, by a host computer operated by a financial institution. In this way, information can be securely exchanged between the card and the remote location using one or more encryption keys that are place in both locations. (Col. 4, lines 15-30)

Such teaching of Carlisle's smart card wherein plurality of accounts is stored and is used in a point-of-sale transaction; encryption which ensures secure communication, wherein the smart card's owner can have confidence in remote installation of services; possessor inserting the smart card into a stand-alone reader equipment, inputting the PIN via the keyboard, and the equipment's display will output the message "OK", thus giving the Holder of the smart card a sense of security that the equipment used for transaction will not capture their PIN string for some future unlawful use and when such stand-alone equipment is unavailable (or when the communication is remote as, for example, when a "dumb" card reader is used the possessor's home), the submitted PIN should be processed in the card and the “OK” message from the smart card should be “time-stamped” and encrypted; logging in, wherein the holder of the smart card can communicate a request for installation of a service offered by a service provider, wherein the service request can be the holder of the smart card requesting the service provider to install money into the smart card ; the smart card which contains an electronic purse that will hold a monetary value and accounts which are implemented by service providers such as Visa, MasterCard, ATM networks, welfare programs, or the like; with the combination of Kawan’s smart card and a smart card reader; allowing the smart card to be validated from a remote location, for example, by a host computer operated by a financial institution; and information which can be securely exchanged between the card and the remote location using one or more encryption keys that are place in both locations are considered “wherein the stored-value account and the credit account were linked to the instrument identifier at a remote host”

Appellant remarks that "the Office Action has provided no reason why in the absence of teachings, the recitations of claims 1 and 30 would be known to one of ordinary skill in the art. As such, the Office Action has failed to meet its *prima facie* burden or proving obviousness". (Argument section, page 9, third paragraph)

The Examiner directs Appellant's attention to the discussions above. Furthermore, in response to Appellant’s remark argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones,* 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation is to improve security. In addition, *KSR* forecloses Appellant's argument that a specific teaching, suggestion, or motivation is required to support a finding of obviousness. *KSR,* 82 USPQ2d at 1396 (2007)

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Marissa Thein/
Examiner, Art Unit 3627

Conferees:

/F. Ryan Zeender/

Supervisory Patent Examiner, Art Unit 3627

/Vincent Millin/

Appeals Practice Specialist, Technology Center 3600